REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

The objection to claim 21 has been corrected herein by amendment, and applicant apologizes for the typographical error.

Claim 9 stands rejected under 35 USC 112, first paragraph, as allegedly failing to comply with the enablement requirement. The rejection alleges that there is no description or example of cards which are "optimized for encryption" of Sonet or ATM cells. However, with all due respect, the specification does in fact describe in detail a card that is optimized for high-speed encryption of Sonet frames. See for example paragraphs 30 and 42-49. These describe the SONET card including

1. Encrypt/Decrypt SONET/SDH FPGA
2. SDRAM for storing the connection table
3. Control CPLD
4. Flash memory for holding the FPGA definitions

The sections clearly describe the manner in which the hardware and the programmed firmware operate to process a

Sonet/SDH frame. A person having ordinary skill in the art would be able to make and use this claimed subject matter without undue experimentation, based on the description of these hardware components.

Analogously, paragraphs 32 and 51-57 describe a card optimized for high-speed operation with ATM cells. This includes the hardware components of:

5. Ingress Cell Processor
6. Egress Cell Processor
7. SDRAM for storing the ingress connection table
8. SDRAM for storing the egress connection table
9. Ingress CAM
10. Egress CAM
11. Encrypt Engine FPGA
12. Decrypt Engine FPGA
13. SDRAM for storing encrypt keys and IV's for each active connection
14. SDRAM for storing decrypt keys and IV's for each active connection
15. Control CPLD
16. SDRAM for holding FPGA definitions

17. High-speed IPSec Processor

These sections also describe the way in which this operates to process a received ATM cell, and provide information that would enable a person having ordinary skill in the art to make and use this claimed subject matter.

Claim 10 stands rejected under 35 USC 112, first paragraph, as allegedly failing to enable the security interlock with memory erasure functions. This contention is respectfully traversed. Claim 22 describes that the keys can be destroyed when power is removed from the encryptor. Paragraph 61 also describes this in additional detail. This requires automatically erasing a memory. Those having ordinary skill in the art would certainly understand that there are various different ways of erasing a memory. For example, when an EEPROM is used, a specified level to the EEPROM will cause its erasure. A keyword search on the patent office web site showed 678 patents relating to this. See for example US patent number 7,099,220, just one of the many hits, which shows different ways of erasing memory. Those having ordinary skill in the art would certainly be able to do this based on the disclosure in the specification in conjunction with the knowledge in the art.

Claims 1-8 and 11-23 stand rejected under 35 USC 102 as allegedly being anticipated by Minear. This contention is respectfully traversed. Claim 1 requires a network encryption system with first and second network interfaces. The first network interface is connected to a protected network, while the second network interface is connected to an unprotected network.

Minear, on the other hand, teaches a firewall, which is always connected to the Internet and always connected in exactly the same way. Minear therefore always connects to the same interface. That interface is a general-purpose network port.

The two interfaces of claim 1, one encrypted and one unencrypted, are nowhere disclosed by Minear. The rejection alleges that the Internet is the unprotected network and the workstations are the protected network. However, Minear only connects to one thing: you can characterize it as an encrypted network or an unencrypted network, but there is only one single type of connection. There is only one way in which Minear is connected: and that is to the Internet. I would characterize this as an unprotected network, whether the workstations were protected or not. However, the only way you get to the

workstations in the first place is via the Internet.

Therefore, Minear does not disclose the two different network interfaces: one of which is adapted for connection to a protected network, the other of which is adapted for connection to an unprotected network. As such, Minear does not anticipate claim 1, because it does not include two separate kinds of network interfaces, of this type.

Claim 1 should hence be allowable along with the dependent claims which depend therefrom. Claim 2 requires FPGAs, which is not disclosed by Minear. The contention that FPGAs are well-known is certainly understood. However, the advantage of FPGAs in an encryption/decryption context is not disclosed by the Microsoft document. Specifically, since FPGAs can be reprogrammed, this allows the high-speed crypto system to be reprogrammed for encryption updates or for different types of encryption operations.

Claim 4 requires a key management subsystem that is separate from the processing part and connected thereto. This is not disclosed by Minear, and in fact, Minear suggests quite the opposite.

The rejection refers to column 5 line 63-64 of Minear. However, this states that "the key management mechanism is in place on the firewall". That means, the firewall itself includes the key management mechanism, not a separate item which communicates via the network.

Column 7 line 22, which was also identified by the official action merely refers about a flag indicating encryption or decryption.

Claim 4 requires a key management subsystem, separate but communicating with the device. There is no teaching or suggestion of using a separate entity for the key management. Therefore, claim 4 should be completely allowable. Claim 5 should be allowable for analogous reasons: as there is no teaching or suggestion of monitoring and managing the keys.

Claim 7 further defines other key management, which is further not disclosed by Minear.

Claim 11 should be further patentable, since it defines using a cryptographic header. Minear refers to the standard

IPsec header that is used to encapsulate packets end to end between two devices. This is a layer 3 encryption which encapsulates an existing packet inside a larger packet. The resulting packet is larger. The expansion of the packet size hence increases the traffic.

In contrast, the present application replaces the header with a cryptographic header and thereby does not require packet expansion.

Claim 12 should be allowable for analogous reasons to those discussed above: including the two networks of different types, and the key management subsystem separated from the networks but connected to thereto by a network protocol.

Claim 22 should be allowable for similar reasons to those discussed above. Claim 22 requires connecting to a first network which is protected and a second network which is unprotected. Claim 22 also defines encrypting data between the networks. This is all not disclosed by Minear. In addition, however, claim 22 defines maintaining the signing key in a separate unit, accessible over a separate network. Minear's figure 4 in column 10 lines 30-52, described the internal

architecture of an operating system. Communication occurs between user space and kernel space using the socket communication method. Operating systems associate sockets with a running process in which the sockets are used to send and receive data. Therefore, if there is vulnerability in the kernel, then all security is internally compromised because there is no physical boundary between the entities. Claim 22 requires a physical separation between the entities, and nowhere is there any disclosure of this in Minear. Claim 22 should hence be allowable.

Claim 23 should be allowable for similar reasons.

Claims 9, 19 and 24 are rejected as allegedly being obvious over Minear in view of Gai. This contention is further respectfully traversed. The rejection combines Minear with Gai in order to use the disclosure of Gai to apply to both ATM and Sonet. In fact, while Gai does teach security groups, it does not appear to teach the specific subject matter of claim 9 which requires a first part for encryption of Sonet and a second part for encryption of ATM.

Moreover, applicants question whether Gai really does

define multiple security types. Gai describes a method of implementing a security group within a network by the application Security Group Tags. In paragraph [0042] Gai states that a packet that includes the SGT may be encrypted.

This is true, but equally the packet may not be encrypted. Whether the packet is or is not encrypted does not depend on the application or otherwise of an SGT. The use of encryption in Gai's Fig 1 is incidental to the use of SGTs. There is no link between the encryption and the tagging of packets such that they may be categorized into security groups.

In fact the only reference in Gai to encryption is in paragraphs [0042] & [0044] stating that a portion of an example packet may or may not be encrypted using any viable method.

In Gai [0044] example packet 107 is encrypted at port 140 then forwarded from router 115 to router 120 (not based upon the SGT). Packet 107 is then decrypted at port 150 of router 120 and the SGT is then checked at egress port 122.

The encryption/decryption of packet 107 occurs entirely between the points in the network at which the SGT is added and

used. The useage of SGTs neither hinders nor requires, indeed is incidental to the encryption or not of the packet.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Attorney's Docket No.: 10824-016001

Applicant asks that all claims be allowed. Please apply the Petition for Extension of Time fee and excess claims fee to Deposit Account No. 06-1050. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: September 5, 2006

Scott C. Harris
Reg. No. 32,030

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

10663276.doc